



CVE-2012-6706

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2012-6706
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-22 13:29:00 UTC
Updated	2018-10-21 10:29:00 UTC
Description	A VMSF_DELTA memory corruption was discovered in unrar before 5.5.5, as used in Sophos Anti-Virus Threat Detection E

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rarlab	Unrar	All	All	All	All
Application	Sophos	Threat Detection Engine	All	All	All	All

References

Reference

- 1286 - VMSF_DELTA filter in unrar allows arbitrary memory write - project-zero - Monorail
- RAR and UnRAR: User-assisted execution of arbitrary code (GLSA 201708-05) — Gentoo security
- McAfee Corporate KB - McAfee Security Bulletin - Web Gateway update fixes vulnerabilities CVE-2012-6706, CVE-2017-1000364, CVE-2017-1000365
- lock.cmpxchg8b.com/sophailv2.pdf
- Sophos Anti-Virus Bugs Let Remote Users Execute Arbitrary Code with Root Privileges and Conduct Cross-Site Scripting Attacks and Let Local Admins Execute Arbitrary Code
- ClamAV: Multiple vulnerabilities (GLSA 201804-16) — Gentoo security
- Sophos products and Tavis Ormandy | Naked Security
- RAR, UnRAR: Multiple vulnerabilities (GLSA 201709-24) — Gentoo Security
- Tavis Ormandy finds vulnerabilities in Sophos Anti-Virus products - Sophos Community
- Sophos Anti-Virus RAR VMSF_DELTA Filter Signedness Error - TELUS Security Labs
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500103](#) Alpine Linux Security Update for clamav

[503827](#) Alpine Linux Security Update for clamav

[710259](#) Gentoo Linux ClamAV Multiple Vulnerabilities (GLSA 201804-16)

[710372](#) Gentoo Linux RAR, UnRAR Multiple Vulnerabilities (GLSA 201709-24)

[710540](#) Gentoo Linux Kodi Arbitrary code execution Vulnerability (GLSA 201710-21)

[710568](#) Gentoo Linux RAR and UnRAR User-assisted execution of arbitrary code Vulnerability (GLSA 201708-05)

[751038](#) SUSE Enterprise Linux Security Update for unrar (SUSE-SU-2021:2834-1)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)